UNIVERSITY OF CALGARY
FACULTY OF SCIENCE

REVISED COURSE OUTLINE FOR REMOTE LEARNING

To account for the necessary transition to remote learning from March 13 onward, adjustments have been made to assessment deadlines and requirements so that all coursework tasks are in line with the necessary and evolving health precautions for all involved (students and staff). If you are unable to meet the deadlines or requirements specified, please connect with your course instructor to work out alternative dates/assessments.

1. **Course:** CPSC 418, Introduction to Cryptography - Winter 2020

   Lecture 01: MWF 14:00 - 14:50 - Remote Learning (check with your instructor or coordinator for details)

Instructor	Email	Phone	Office	Hours
Dr. Renate Scheidler	rscheidl@ucalgary.ca	220-6628	MS 436	MW 15:30-16:30 via Zoom https://ucalgary.zoom.us/j/630043479

   Course Site:

   D2L: CPSC 418 & MATH 318 L01-(Winter 2020)-Introduction to Cryptography

   Note: Students must use their U of C account for all course correspondence.

   Course web page: people.ucalgary.ca/~rscheidl/418

2. **Requisites:**

   See section 3.5.C in the Faculty of Science section of the online Calendar.

   Prerequisite(s):
   Computer Science 331; and one of Mathematics 271, 273, 315 or Pure Mathematics 315.

   Antirequisite(s):
   Credit for Computer Science 418 and any of Computer Science 429, 557, Mathematics 318, Pure Mathematics 329 or 418 will not be allowed.

   Note(s):
   a. Students who have credit for Computer Science 319 instead of Computer Science 331 Computer Science should contact the department for instructions on how to enrol in this course.

3. **Grading:**

   The University policy on grading and related matters is described in F.1 and F.2 of the online University Calendar. In determining the overall grade in the course the following weights will be used:

Component(s)	Weighting %	Date
Assignments (3)	30	(Due dates: February 12, March 14, April 18)
Midterm Exam (1)	30	(Online March 18)
Final Exam	40	(Take-home, due 11:30am, April 28)

   Each piece of work (reports, assignments, quizzes, midterm exam(s) or final examination) submitted by the student will be assigned a grade. The student's grade for each component listed above will be combined with the indicated weights to produce an overall percentage for the course, which will be used to determine the course letter grade.

   The conversion between a percentage grade and letter grade is as follows.

	A+	A	A-	B+	B	B-	C+	C	C-	D+	D
Minimum % Required	95 %	90 %	86 %	82%	78%	74 %	70 %	66%	62%	58 %	50 %

   A passing grade in the final exam (at least 50%) is essential if the student is to pass the course as a whole (grade of C- or better).

4. **Missed Components Of Term Work:**

The University has suspended requirements for students to provide evidence for reasons for absences so please do not attend medical clinics for medical notes or Commissioners for Oaths for statutory declarations. Please let your instructor know immediately if you are ill and cannot meet the deadlines specified.

5. **Scheduled Out-of-Class Activities:**

The following out of class activities are scheduled for this course.

Activity	Location	Date and Time	Duration
Out of Class Midterm	ST 148	Wednesday, March 18, 2020 at 6:00 pm	90 Minutes

REGULARLY SCHEDULED CLASSES HAVE PRECEDENCE OVER ANY OUT-OF-CLASS-TIME-ACTIVITY. If you have a conflict with the out-of-class-time-activity, please contact your course coordinator/instructor no later than **14 days prior** to the date of the out-of-class activity so that alternative arrangements may be made.

6. **Course Materials:**

Recommended Textbook(s):

D. R. Stinson and M. B. Paterson,*Cryptography - Theory and Practice*: CRC 2019.

Additional course materials such as lecture slides, assignments, handouts and links to useful resources are available on the course website.

7. **Examination Policy:**

No aids of any kind are allowed on tests or examinations.

Students should also read the Calendar, Section G, on Examinations.

8. **Approved Mandatory And Optional Course Supplemental Fees:**

There are no mandatory or optional course supplemental fees for this course

9. **Writing Across The Curriculum Statement:**

For all components of the course, in any written work, the quality of the student's writing (language, spelling, grammar, presentation etc.) can be a factor in the evaluation of the work. See also Section E.2 of the University Calendar.

10. **Human Studies Statement:**

Students will not participate as subjects or researchers in human studies.

See also Section E.5 of the University Calendar.

11. **Reappraisal Of Grades:**

A student wishing a reappraisal, should first attempt to review the graded work with the Course coordinator/instructor or department offering the course. Students with sufficient academic grounds may request a reappraisal. Non-academic grounds are not relevant for grade reappraisals. Students should be aware that the grade being reappraised may be raised, lowered or remain the same. See Section I.3 of the University Calendar.

   a. **Term Work:** The student should present their rationale as effectively and as fully as possible to the Course coordinator/instructor within **ten business days** of either being notified about the mark, or of the item's return to the class. If the student is not satisfied with the outcome, the student shall submit the Reappraisal of Graded Term work form to the department in which the course is offered within 2 business days of receiving the decision from the instructor. The Department will arrange for a reappraisal of the work within the next ten business days. The reappraisal will only be considered if the student provides a detailed rationale that outlines where and for what reason an error is suspected. See sections I.1 and I.2 of the University Calendar

   b. **Final Exam:** The student shall submit the request to Enrolment Services. See Section I.3 of the University Calendar.

12. **Other Important Information For Students:**

   a. **Mental Health** The University of Calgary recognizes the pivotal role that student mental health plays in physical health, social connectedness and academic success, and aspires to create a caring and supportive

campus community where individuals can freely talk about mental health and receive supports when needed. We encourage you to explore the mental health resources available throughout the university community, such as counselling, self-help resources, peer support or skills-building available through the SU Wellness Centre (Room 370, MacEwan Student Centre, [Mental Health Services Website](#)) and the Campus Mental Health Strategy website ([Mental Health](#)).

b. **SU Wellness Center:** The Students Union Wellness Centre provides health and wellness support for students including information and counselling on physical health, mental health and nutrition. For more information, see [www.ucalgary.ca/wellnesscentre](#) or call [403-210-9355](#).

c. **Sexual Violence:** The University of Calgary is committed to fostering a safe, productive learning environment. The Sexual Violence Policy [(https://www.ucalgary.ca/policies/files/policies/sexual-violence-policy.pdf)](#) is a fundamental element in creating and sustaining a safer campus environment for all community members. We understand that sexual violence can undermine students' academic success and we encourage students who have experienced some form of sexual misconduct to talk to someone about their experience, so they can get the support they need. The Sexual Violence Support Advocate, Carla Bertsch, can provide confidential support and information regarding sexual violence to all members of the university community. Carla can be reached by email ([svsa@ucalgary.ca](#)) or phone at [403-220-2208](#) .

d. **Misconduct:** Academic misconduct (cheating, plagiarism, or any other form) is a very serious offence that will be dealt with rigorously in all cases. A single offence may lead to disciplinary probation or suspension or expulsion. The Faculty of Science follows a zero tolerance policy regarding dishonesty. Please read the sections of the University Calendar under [Section K](#). Student Misconduct to inform yourself of definitions, processes and penalties. Examples of academic misconduct may include: submitting or presenting work as if it were the student's own work when it is not; submitting or presenting work in one course which has also been submitted in another course without the instructor's permission; collaborating in whole or in part without prior agreement of the instructor; borrowing experimental values from others without the instructor's approval; falsification/ fabrication of experimental values in a report. **These are only examples**.

e. **Assembly Points:** In case of emergency during class time, be sure to FAMILIARIZE YOURSELF with the information on [assembly points](#).

f. **Academic Accommodation Policy:** Students needing an accommodation because of a disability or medical condition should contact Student Accessibility Services in accordance with the procedure for accommodations for students with disabilities available at [procedure-for-accommodations-for-students-with-disabilities.pdf](#).

Students needing an accommodation in relation to their coursework or to fulfill requirements for a graduate degree, based on a protected ground other than disability, should communicate this need, preferably in writing, to the Associate Head of Undergraduate Affairs of the Department of Computer Science, Nathaly Verwaal by email nmverwaa@ucalgary.ca or phone 403-220-8485. Religious accommodation requests relating to class, test or exam scheduling or absences must be submitted no later than **14 days** prior to the date in question. See [Section E.4](#) of the University Calendar.

g. **Safewalk:** Campus Security will escort individuals day or night (See the [Campus Safewalk](#) website). Call [403-220-5333](#) for assistance. Use any campus phone, emergency phone or the yellow phones located at most parking lot pay booths.

h. **Freedom of Information and Privacy:** This course is conducted in accordance with the Freedom of Information and Protection of Privacy Act (FOIPP). Students should identify themselves on all written work by placing their name on the front page and their ID number on each subsequent page. For more information, see [Legal Services](#) website.

i. **Student Union Information:** [VP Academic](#), Phone: [403-220-3911](#) Email: [suvpaca@ucalgary.ca](#). SU Faculty Rep., Phone: [403-220-3913](#) Email: [sciencerep@su.ucalgary.ca](#). [Student Ombudsman](#), Email: [ombuds@ucalgary.ca](#).

j. **Internet and Electronic Device Information:** Unless instructed otherwise, cell phones should be turned off during class. All communication with other individuals via laptop, tablet, smart phone or other device is prohibited during class unless specifically permitted by the instructor. Students that violate this policy may be asked to leave the classroom. Repeated violations may result in a charge of misconduct.

k. **Surveys:** At the University of Calgary, feedback through the Universal Student Ratings of Instruction ([USRI](#)) survey and the Faculty of Science Teaching Feedback form provides valuable information to help with evaluating instruction, enhancing learning and teaching, and selecting courses. Your responses make a

difference - please participate in these surveys.

l. **Copyright of Course Materials:** All course materials (including those posted on the course D2L site, a course website, or used in any teaching activity such as (but not limited to) examinations, quizzes, assignments, laboratory manuals, lecture slides or lecture materials and other course notes) are protected by law. These materials are for the sole use of students registered in this course and must not be redistributed. Sharing these materials with anyone else would be a breach of the terms and conditions governing student access to D2L, as well as a violation of the copyright in these materials, and may be pursued as a case of student academic or non-academic misconduct, in addition to any other remedies available at law.

Course Outcomes:
- Describe the different services that cryptography provides and give examples of cryptographic mechanisms that provide a given service.
- Verify that a cryptographic mechanism works properly, eg. that encryption followed by decryption is successful.
- Describe the different attack models covered in the course and how they relate to each other.
- Demonstrate competence with mathematical foundations of modern cryptographic primitives.
- Apply mathematics to assess the security of cryptographic primitives.
- Restate the main cryptographic protocols that are covered in the course and their different functions.
- Write software that provides cryptographic services and integrate existing cryptographic software libraries and packages in this software.

Electronically Approved - Mar 19 2020 09:00

Department Approval

Electronically Approved - Mar 20 2020 16:55

Associate Dean's Approval for alternate final examination arrangements or remote learning and out of regular class-time activity